Zuständigkeiten	Rollen
Grundsätzlich zuständig	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeitende, IT-Betrieb, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.10.A1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen (B) [Haustechnik, IT-Betrieb]

In den Räumen vorhandene Gerätschaften MÜSSEN angemessen gegen Diebstahl gesichert werden. Zudem MUSS festgelegt werden, wer die in den Räumen dauerhaft vorhandenen IT- und sonstigen Systeme administriert. Es MUSS auch festgelegt werden, ob und unter welchen Bedingungen von externen Personen mitgebrachte IT-Systeme verwenden dürfen. Weiterhin MUSS festgelegt werden, ob und auf welche Netzzugänge und TK-Schnittstellen externen Personen zugreifen dürfen.

INF.10.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

INF.10.A3 Geschlossene Fenster und Türen (B) [Mitarbeitende]

Die Fenster und Türen der Besprechungs-, Veranstaltungs- und Schulungsräume MÜSSEN beim Verlassen verschlossen werden. Bei Räumlichkeiten, in denen sich IT-Systeme oder schützenswerte Informationen befinden, MÜSSEN die Türen beim Verlassen abgeschlossen werden. Zusätzlich MUSS regelmäßig geprüft werden, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.10.A4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen (S)

Bei der Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen SOLLTE besonders die Lage der Räume berücksichtigt werden. Insbesondere Räumlichkeiten, die oft zusammen mit oder ausschließlich von externen Personen genutzt werden, SOLLTEN NICHT in Gebäudeteilen liegen, in deren Nähe regelmäßig vertrauliche Informationen besprochen und bearbeitet werden. Es SOLLTE für jeden Raum festgelegt werden, wie vertraulich die Informationen sein dürfen, die dort besprochen oder verarbeitet werden.

INF.10.A5 Fliegende Verkabelung (S)

Die Stromanschlüsse SOLLTEN sich dort befinden, wo Beamer, Laptops oder andere elektronische Geräte aufgestellt werden. Verkabelungen, die über den Boden verlaufen, SOLLTEN geeignet abgedeckt werden.

INF.10.A6 Einrichtung sicherer Netzzugänge (S) [IT-Betrieb]

Es SOLLTE sichergestellt werden, dass mitgebrachte IT-Systeme nicht über das Datennetz mit internen IT-Systemen der Institution verbunden werden können. Auf das LAN der Institution SOLLTEN ausschließlich dafür vorgesehene IT-Systeme zugreifen können. Ein Datennetz für externe Personen SOLLTE vom LAN der Institution getrennt werden. Netzzugänge SOLLTEN so eingerichtet sein, dass verhindert wird, dass Dritte den internen Datenaustausch mitlesen können. Netzanschlüsse in Besprechungs-, Veranstaltungs- oder Schulungsräumen SOLLTEN abgesichert werden. Es SOLLTE verhindert werden, dass IT-Systeme in Besprechungs-, Veranstaltungs- und Schulungsräumen gleichzeitig eine Verbindung zum Intranet und zum Internet aufbauen können.

Außerdem SOLLTE die Stromversorgung aus einer Unterverteilung heraus getrennt von anderen Räumen aufgebaut werden.

INF.10.A7 Sichere Konfiguration von Schulungs- und Präsentationsrechnern (S) [IT-Betrieb]

Dedizierte Schulungs- und Präsentationsrechner SOLLTEN mit einer Minimalkonfiguration versehen werden. Es SOLLTE festgelegt sein, welche Anwendungen auf Schulungs- und Präsentationsrechnern in der jeweiligen Veranstaltung genutzt werden können. Die Schulungs- und Präsentationsrechner SOLLTEN nur an ein separates, vom LAN der Institution getrenntes Datennetz angeschlossen werden.

INF.10.A8 Erstellung eines Nutzungsnachweises für Räume (S)

Je nach Nutzungsart der Besprechungs-, Veranstaltungs- und Schulungsräume SOLLTE ersichtlich sein, wer die Räume zu welchem Zeitpunkt genutzt hat. Für Räumlichkeiten, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen durchgeführt werden, SOLLTEN ebenfalls Nutzungsnachweise erbracht werden. Es SOLLTE überlegt werden, für Räumlichkeiten, die für jeden Mitarbeitenden zugänglich sind, ebenfalls entsprechende Nutzungsnachweise einzuführen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.10.A9 Zurücksetzen von Schulungs- und Präsentationsrechnern (H) [IT-Betrieb]

Es SOLLTE ein Verfahren festgelegt werden, um Schulungs- und Präsentationsrechner nach der Nutzung auf einen vorher definierten Zustand zurückzusetzen. Durch von Benutzenden durchgeführte Änderungen SOLLTEN dabei vollständig entfernt werden.

INF.10.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.11 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden und Räumen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel CF19 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm DIN EN 1627-1630:2021-11 Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.11 Allgemeines Fahrzeug

1. Beschreibung

1.1. Einleitung

Institutionen nutzen in vielen Situationen die unterschiedlichsten Fahrzeuge im Nah- und Fernbereich. Als Fahrzeug werden im Kontext dieses Bausteins motorisierte Fortbewegungsmittel bezeichnet, die sich in der Regel auf Land- und Luftstraßen, Seewegen sowie Wasserstraßen bewegen und über eine Fahrzeugkabine oder Vergleichbares verfügen. Beispiele hierfür sind PKW, LKW, Flugzeuge oder Schiffe. Im folgenden Text wird nur noch der Oberbegriff Fahrzeug verwendet, außer es ist eine bestimmte Art von Fahrzeug gemeint.

Nahezu alle modernen Fahrzeuge verfügen über integrierte IT-Komponenten, wie zum Beispiel Infotainmentsysteme oder interne Analysesysteme, die im Rahmen der Informationssicherheit ganzheitlich betrachtet werden müssen. Darüber hinaus werden dienstliche Aufgaben häufig nicht nur in den Räumen und Gebäuden einer Institution erledigt, sondern auch innerhalb von Fahrzeugen, die sich an wechselnden Standorten und in verschiedenen Umgebungen befinden können. Ein Fahrzeug ist somit auch eine eigenständige mobile Arbeitsumgebung, die durch die Institution angemessen abgesichert werden muss.

1.2. Zielsetzung

Der Baustein beschreibt spezifische Gefährdungen, die zu beachten sind, wenn Institutionen Fahrzeuge mit IT-Komponenten einsetzen oder Fahrzeuge im Allgemeinen als IT-Arbeitsplätze verwenden. Darauf aufbauend legt der Baustein fest, welche Anforderungen von Fahrzeugnutzenden und -haltenden zu erfüllen sind, um den optimalen Betrieb eines Fahrzeugs aus Sicht der Informationssicherheit zu gewährleisten.

1.3. Abgrenzung und Modellierung

Der Baustein INF.11 *Allgemeines Fahrzeug* ist grundsätzlich auf jedes von der Institution eingesetztes Land-, Luft- und Wasserfahrzeug einmal anzuwenden.

Adressaten des Bausteins sind Benutzende und Betreibende von Fahrzeugen. Autonom fahrende oder ferngesteuerte Fahrzeuge, Schienenfahrzeuge und Raumfahrzeuge sind von diesem Baustein ausgenommen.

Die Art, die Ausstattung, der Einsatzort und das Aufgabenfeld von Fahrzeugen können sich je nach Institution voneinander unterscheiden. In dem Baustein INF.11 *Allgemeines Fahrzeug* werden nur die typischen Einsatzszenarien von Fahrzeugen berücksichtigt, sodass spezielle Einsatzzwecke, wie etwa Rettungseinsätze von Rettungshubschraubern oder Kampfeinsätze von Militärfahrzeugen, ergänzend individuell betrachtet werden müssen.

Daher wird nicht abschließend auf nachträglich eingebaute, einsatzspezifische IT-Systeme oder fahrzeugspezifische Fachanwendungen eingegangen, wie sie zum Beispiel bei Einsatzfahrzeugen oder Führungsfahrzeugen üblich sind. Die Ausstattung und die damit verbundenen Fachanwendungen dieser Fahrzeuge sind individuell ergänzend zu behandeln.

Außerdem werden die fahrzeugeigenen Netze über Kommunikationsbusse wie CAN, LIN oder Flexray, auch IVN (In-Vehicle-Network) genannt, nicht betrachtet, da diese in der Regel nicht durch die Anwendenden verändert werden.

Um die mitgeführten und nachträglich eingebauten IT-Komponenten abzusichern, müssen alle relevanten Bausteine, wie SYS.3.1 *Laptops*, SYS.3.2 *Allgemeine Smartphones und Tablets*, NET.3.3 *VPN* und die Bausteinschichten NET.4 *Telekommunikation* sowie NET.2 *Funknetze* gesondert berücksichtigt werden.

Darüber hinaus muss, bevor das Fahrzeug entsorgt, bzw. ausgesondert wird, der Baustein CON.6 *Löschen und Vernichten* angewendet werden, damit keine schützenswerten Informationen im Fahrzeug verbleiben.

Dieser Baustein behandelt alle infrastrukturellen Aspekte, sodass INF.9 *Mobiler Arbeitsplatz* nicht zusätzlich zu modellieren ist.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.11 *Allgemeines Fahrzeug* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für Fahrzeuge

Wird nicht oder nur unzureichend geregelt, welche Informationen über die von Fahrzeugen für Benutzende zur Verfügung gestellten Netze wie WLAN oder Bluetooth übertragen und verarbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind, können vertrauliche Informationen offengelegt werden. Wird nicht hinreichend geregelt, wie diese abzusichern und zu benutzen sind, könnten schützenswerte Informationen wie personenbezogene Daten offengelegt werden.

Wenn Fahrzeuge gestohlen werden oder integrierte IT-Komponenten ausfallen und es hierfür keine Regelungen und festgelegte Abläufe gibt, kann dies gravierende Folgen haben. Es besteht die Gefahr, dass schützenswerte Informationen im Fahrzeug verbleiben und unbefugte Dritte Zugang zu diesen erhalten.

Wenn Fahrzeuge oder die darin verbauten IT-Komponenten unsachgemäß in Betrieb genommen werden, kann dies zu umfangreichen Gefährdungen der Informationssicherheit führen. Es könnten relevante Einstellungen, wie die automatische Synchronisation von Telefonbüchern, falsch konfiguriert sein oder es könnten Funktionstest bei Flugzeugen übersprungen oder unsachgemäß durchgeführt werden. Dies wiederum kann dazu führen, dass die Systeme des Flugzeuges während des Einsatzes nicht wie vorgesehen funktionieren und schlimmstenfalls zu einem Totalverlust des Flugzeugs führen.

Genauso kann aber auch die Funktion der integrierten IT-Komponenten und des gesamten Fahrzeuges gefährdet werden, wenn das Fahrzeug unsachgemäß ausgeschaltet oder temporär außer Betrieb genommen wird. Ein Beispiel hierfür sind Einsatzfahrzeuge. Werden diese für einen längeren Zeitraum ausgeschaltet, so droht aufgrund der umfangreichen Ausstattung, dass sich die Fahrzeugbatterie vollständig entlädt. Infolgedessen kann das Fahrzeug nicht mehr starten und in den integrierten IT-Komponenten könnten Daten verloren gehen.

2.2. Fehlendes Sicherheitsbewusstsein und Sorglosigkeit beim Umgang mit dem Fahrzeug

Fehlendes Sicherheitsbewusstsein und Sorglosigkeit beim Umgang mit den Fahrzeugen und deren Komponenten stellen eine ernstzunehmende Gefahr dar. Sind Mitarbeitende beispielsweise nicht ausreichend geschult, wie sie mit den Fahrzeugen und den IT-Komponenten umgehen sollen und sind sich der möglichen Risiken nicht bewusst, könnten Fahrzeuge und die darin verbauten IT-Komponenten falsch oder unsorgfältig benutzt werden. So werden zum Beispiel IT-Systeme auf Brücken von Schiffen von unterschiedlichen Personen benutzt. Werden nun wesentliche Einstellungen von einem Benutzenden verändert, ohne die weiteren Benutzenden darüber zu informieren, dann könnten Fehlfunktionen auftreten, die die weiteren Benutzenden nicht nachvollziehen können.

Eine weitere Gefahr kann darin bestehen, dass Fahrzeuge unzuverlässig abgeschlossen werden. Hierdurch könnten unbefugte Dritte einfach die Fahrzeugkabine betreten und alle dort vorhandenen IT-Komponenten und abgelegten Informationen einsehen oder entwenden.

Weiterhin könnten schlecht geschulte Mitarbeitende unangemessen auf Störungen reagieren und durch eine falsche Reaktion die Situation verschlimmern. Wird z. B. bei einer Störung der integrierten IT-Systeme des Fahrzeugs nicht die hierfür zuständige Stelle der Institution kontaktiert, sondern vom Benutzenden versucht, die Störung selbst zu beheben, können hieraus unabsehbare Folgen resultieren. Es könnten beispielsweise relevante Einstellungen für die Sicherheit oder den Datenschutz verändert werden.

2.3. Ungeregelte Datenübertragung an Dritte und unsichere Kommunikationsschnittstellen

Viele moderne Fahrzeuge verfügen nicht nur über die für die Benutzenden relevanten bzw. direkt ersichtlichen drahtlosen Kommunikationsschnittstellen, wie z. B. Bluetooth oder WLAN. Viele interne Systeme des Fahrzeugs kommunizieren direkt über integrierte Mobilfunkschnittstellen mit IT-Systemen der herstellenden Unternehmen, wobei dieser Informationsaustausch von den Anwendenden in der Regel nicht beeinflusst werden kann. Hiermit sind nicht nur gesetzlich vorgeschriebene und für den Anwendenden transparente Systeme wie der eCall gemeint, sondern insbesondere auch solche, die nicht für den Benutzenden direkt ersichtlich sind. Beispielsweise übertragen viele fahrzeugherstellende Unternehmen Daten, um detaillierte Informationen über den Standort und die Kilometerzahl des Fahrzeugs oder über das Verhalten der Fahrzeugführenden zu sammeln. Dadurch könnten umfangreich personenbezogene Daten über die Fahrzeugnutzenden erhoben werden, ohne dass diese darüber Kenntnis haben oder dieser Datenerhebung und -verarbeitung explizit zugestimmt haben.

Eine weitere Gefahr sind unsichere Kommunikationsschnittstellen der Fahrzeuge. Durch mangelnde Schutzmechanismen können so sensible Daten ausgelesen werden. Lässt beispielsweise das Infotainmentsystem eine Bluetooth-Koppelung ohne Sicherheitsmechanismen zu, könnten unbefugte Dritte ihr Smartphone unbemerkt damit koppeln und Adressbücher synchronisieren.

2.4. Unsachgemäße Veränderungen am Fahrzeug

Während herkömmliche PKW sehr selten durch den Fahrzeugbetreibenden verändert werden, müssen Fahrzeuge für spezialisierte Einsatzzwecke sehr häufig noch durch die Betreibenden oder spezialisierten Unternehmen nachträglich angepasst werden. Ein Beispiel hierfür sind Einsatzfahrzeuge oder nachträglich modernisierte oder umfunktionierte Schiffe. Wird in diesen Fällen ein Fahrzeug unsachgemäß verändert, indem z. B. zusätzliche Kabel ungeeignet verlegt werden, kann dies zu erheblichen Schäden bis hin zum Totalverlust des Fahrzeugs führen.

Auch anderweitige Veränderungen können die Einsatzfähigkeit der Fahrzeuge beeinträchtigen. Wird z. B das Infotainmentsystem manipuliert, um neue bzw. gesperrte Funktionen freizuschalten, könnten die Updates des herstellenden Unternehmens nicht mehr eingespielt und damit verbunden potentielle Sicherheitslücken nicht mehr geschlossen werden.

2.5. Manipulation, unbefugter Zutritt und Diebstahl bei Fahrzeugen

Offen in Fahrzeugen liegende Informationen können häufig von außerhalb der Fahrzeuge eingesehen werden, wenn kein oder nur ein unzureichender Sichtschutz vorhanden ist. Dies kann Begehrlichkeiten wecken, die zu Angriffen führen.

Fahrzeuge werden häufig auf öffentlich zugänglichen Parkplätzen abgestellt oder an Bootsanlegern vertäut, die nicht durch zentrale Schutzmaßnahmen der Institution, wie Sicherheitsdienste oder verschlossene Garagen, geschützt werden. Sie sind somit prinzipiell einem erhöhten Risiko ausgesetzt, von Unbefugten betreten zu werden. Unsichere Schließsysteme können hierbei eine Schwachstelle sein. Zum Beispiel können sogenannte schlüssellose Schließsysteme an Fahrzeugen unter Umständen leicht durch Relay-Angriffe umgangen werden.

Somit können IT-Systeme, Zubehör, Informationen und Software häufig einfacher manipuliert, zerstört oder gestohlen werden, wenn sie in Fahrzeugen statt in Räumlichkeiten der Institution unbeaufsichtigt aufbewahrt werden. Werden IT-Systeme, Zubehör, Informationen oder Software manipuliert oder zerstört, sind die Mitarbeitenden in Fahrzeugen oft nur noch eingeschränkt arbeitsfähig. Die betroffenen IT-Systeme könnten sogar in der Art manipuliert werden, dass z. B. die darauf verarbeiteten Daten durch Schadsoftware an unbefugte Dritte weitergeleitet werden. Des Weiteren müssen womöglich zerstörte IT-Komponenten ersetzt werden, was sowohl finanzielle als auch personelle Ressourcen erfordert.

2.6. Gefahren im Zusammenhang mit Wartung, Reparatur und Updates

Werden Fahrzeuge und die verwendeten IT-Komponenten nicht oder nur unzureichend gewartet und gepflegt oder ihre Funktionsfähigkeit nicht regelmäßig überprüft, kann das dazu führen, dass sie im Bedarfsfall nicht oder nur eingeschränkt einsatzfähig sind.

Eine große Herausforderung hierbei ist, dass Updates für die in den Fahrzeugen integrierten IT-Systeme nicht unbedingt zu den regelmäßigen Wartungszyklen der Fahrzeuge bereitstehen. Dadurch könnten Updates beispielsweise nur unregelmäßig und verzögert eingespielt werden.

In institutionseigenen Werkstätten können die Fahrzeuge und die verbauten IT-Komponenten in der Regel nicht vollständig gewartet oder repariert werden, weshalb Fahrzeuge häufig an Fremdfirmen übergeben werden. In den Räumlichkeiten der Fremdfirmen sind die Fahrzeuge meist unbeobachtet und Dritte können umfassend auf das Fahrzeug und die verwendeten IT-Komponenten zugreifen. Dadurch besteht ein erhöhtes Risiko, dass die IT-Komponenten missbraucht oder schützenswerte Informationen entwendet werden.

2.7. Gefahren bei der Aussonderung

Werden Fahrzeuge ausgesondert, können diese mit allen verbauten IT-Komponenten oder mit einem Teil davon veräußert werden. Hierdurch können Fremdpersonen auf die IT-Komponenten zugreifen und so auf interne Informationen oder personenbezogene Daten rückschließen, wie zum Beispiel gespeicherte Telefonnummern. Außerdem können institutionseigene Komponenten wie SIM-Karten oder Kryptomodule in den Fahrzeugen verbleiben. Somit würden die nachfolgenden Besitzenden ungewollt Zugang zu diesen erhalten und könnten beispielsweise Informationen aus diesen Komponenten auslesen (wie z. B. Telefonnummern von der SIM-Karte) und widerrechtlich verwenden.

2.8. Unzulässige Temperatur und Luftfeuchte in Fahrzeugen

Jedes Gerät hat einen Temperaturbereich, innerhalb dessen es ordnungsgemäß funktioniert. Über- oder unterschreitet die Raumtemperatur die Grenzen dieses Bereiches, können Geräte sowie IT-Komponenten ausfallen und der Betrieb kann gestört werden. Ähnliches gilt für die Luftfeuchtigkeit. In Fahrzeugen liegen unterschiedliche Voraussetzungen vor, die genau zu solchen Situationen führen können. So kann der Innenraum von in der Sonne abgestellten Fahrzeugen bis zu 70 Grad erreichen und somit den üblichen Temperaturbereich von z. B. Lithium-Ionen-Akkus überschreiten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.11 *Allgemeines Fahrzeug* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte
Weitere Zuständigkeiten	Mitarbeitende, Fachverantwortliche, Datenschutzbeauftragte, Benutzende, Beschaffungsstelle, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.11.A1 Planung und Beschaffung (B) [Fachverantwortliche, Beschaffungsstelle, Datenschutzbeauftragte]

Bevor Fahrzeuge beschafft werden, MUSS der Einsatzzweck geplant werden. Die funktionalen Anforderungen an die Fahrzeuge und insbesondere die Anforderungen an die Informationssicherheit, sowie den Datenschutz der verbauten IT-Komponenten MÜSSEN erhoben werden. Hierbei MÜSSEN folgende Aspekte berücksichtigt werden:

- Einsatzszenarien der Fahrzeuge,
- nähere Einsatzumgebung der Fahrzeuge sowie
- der gesamte Lebenszyklus der Fahrzeuge.

Die Fahrzeuge MÜSSEN außerdem über angemessene Schließsysteme verfügen, sofern die Fahrzeuge nicht durchgehend durch andere Maßnahmen oder Regelungen gesichert werden können. Während der Planung SOLLTE berücksichtigt werden, dass viele Fahrzeuge Daten an die fahrzeugherstellenden Unternehmen und weitere Dritte übermitteln können.

INF.11.A2 Wartung, Inspektion und Updates (B) [Fachverantwortliche, IT-Betrieb]

Die Fahrzeuge und die dazugehörenden IT-Komponenten MÜSSEN nach den Vorgaben des herstellenden Unternehmens gewartet werden. Hierbei MUSS beachtet werden, dass die Intervalle der herkömmlichen Wartung und von Updates der integrierten IT-Komponenten voneinander abweichen können. Es MUSS klar geregelt werden, wer in welcher Umgebung die Updates installieren darf. Auch „Over-the-Air" (OTA) Updates MÜSSEN geregelt eingespielt werden.

Wartungs- und Reparaturarbeiten MÜSSEN von befugtem und qualifiziertem Personal in einer sicheren Umgebung durchgeführt werden. Dabei SOLLTE schon vor der Wartung geklärt werden, wie mit Fremdfirmen umgegangen wird. Werden Fahrzeuge in fremden Institutionen gewartet, SOLLTE geprüft werden, ob alle nicht benötigten, zum Fahrzeug dazugehörigen portablen IT-Systeme entfernt werden.

Werden die Fahrzeuge wieder in den Einsatzbetrieb integriert, MUSS mittels Checkliste geprüft werden, ob alle Beanstandungen und Mängel auch behoben wurden. Es MUSS auch geprüft werden, ob die vorhandenen IT-Komponenten einsatzfähig sind.

INF.11.A3 Regelungen für die Fahrzeugbenutzung (B) [IT-Betrieb, Fachverantwortliche, Benutzende, Datenschutzbeauftragte]

Für alle Tätigkeiten, die sich auf die Sicherheit der in den Fahrzeugen verarbeiteten Informationen auswirken können, MUSS vorher geregelt werden, ob sie in den Fahrzeugen durchgeführt werden dürfen. Hierbei MUSS klar geregelt werden, welche Informationen dabei transportiert und bearbeitet werden dürfen. Ergänzend MUSS festgelegt werden, welche Schutzvorkehrungen dabei zu treffen sind. Dies MUSS für jede Art von Information gelten, auch für Gespräche in den Fahrzeugen. Es MUSS geklärt werden, unter welchen Rahmenbedingungen Mitarbeitende auf welche Art von Informationen ihrer Institution zugreifen dürfen.

Außerdem MUSS geregelt werden, in welchem Umfang Infotainmentsysteme, Anwendungen und sonstige Services der Fahrzeuge genutzt werden dürfen. Des Weiteren MUSS festgelegt werden, wie Schnittstellen abzusichern sind. In bestehende Geschäfts- bzw. Dienstanweisungen MUSS beschrieben werden, wie mitgeführte IT in den Fahrzeugen verwendet und aufbewahrt werden darf.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.11.A4 Erstellung einer Sicherheitsrichtlinie (S) [Fachverantwortliche, IT-Betrieb]

Alle relevanten Sicherheitsanforderungen für die IT innerhalb der Fahrzeuge SOLLTEN in einer für Mitarbeitende verpflichtenden Sicherheitsrichtlinie dokumentiert werden. Die Richtlinie SOLLTE allen relevanten Mitarbeitenden der Institution bekannt sein und die Grundlage für ihren Umgang mit Fahrzeugen darstellen. In der Richtlinie SOLLTEN die Zuständigkeiten für einzelne Aufgaben klar geregelt sein. Die Sicherheitsrichtlinie SOLLTE regelmäßig überprüft und anlassbezogen aktualisiert werden.

INF.11.A5 Erstellung einer Inventarliste (S)

Für jedes Fahrzeug SOLLTE eine Inventarliste über

- die im Fahrzeug fest verbauten oder zugehörigen IT-Komponenten (z. B. Handfunkgeräte bei Einsatzfahrzeugen),
- die Fachverfahren, die auf den integrierten IT-Komponenten ausgeführt werden,
- Handlungsanweisungen und Betriebsdokumentationen sowie
- die mit dem Infotainmentsystem gekoppelten Mobilgeräte

geführt werden. Die Inventarliste SOLLTE regelmäßig und anlassbezogen aktualisiert werden. Dabei SOLLTE überprüft werden, ob noch alle inventarisierten zum Fahrzeug gehörenden IT-Komponenten vorhanden sind. Zusätzlich

SOLLTE anhand der Inventarliste überprüft werden, ob keine mobilen Endgeräte unerlaubt mit dem Infotainmentsystem gekoppelt worden sind.

INF.11.A6 Festlegung von Handlungsanweisungen (S) [Fachverantwortliche, Benutzende]

Für alle wesentlichen Situationen, die die Informationssicherheit von Fahrzeugen betreffen, SOLLTEN Handlungsanweisungen in Form von Checklisten vorliegen. Die Handlungsanweisungen SOLLTEN dabei in die Sicherheitsrichtlinie integriert werden und in geeigneter Form als Checklisten verfügbar sein, während das Fahrzeug benutzt wird. Hierbei SOLLTE auch der Fall berücksichtigt werden, dass das Fahrzeug selbst gestohlen wird. Die Handlungsanweisungen SOLLTEN insbesondere nachfolgende Szenarien behandeln:

- Ausfall von IT-Komponenten der Fahrzeuge,
- Notfallsituationen wie Unfälle,
- unerlaubtes Betreten der Fahrzeuge sowie
- Diebstahl der Fahrzeuge oder darin abgelegter Gegenstände mit Relevanz für die Informationssicherheit.

Die Zuständigkeiten für die einzelnen Aufgaben SOLLTEN in der Checkliste dokumentiert sein. Die Anweisungen SOLLTEN von den Fahrzeugbenutzenden in den entsprechenden Situationen angewendet werden. Anhand der Checkliste SOLLTE dokumentiert werden, wie sie in diesen Situationen vorgegangen sind.

INF.11.A7 Sachgerechter Umgang mit Fahrzeugen und schützenswerten Informationen (S) [Fachverantwortliche, Benutzende]

Die Institution SOLLTE die Handlungsanweisungen zur Fahrzeugbenutzung um Aspekte ergänzen, wann, wie und wo Fahrzeuge sachgerecht abgestellt bzw. angedockt werden dürfen. Hierbei SOLLTE primär die Frage beantwortet werden, welche Umgebungen die Fahrzeuge angemessenen vor unerlaubten Zutritt oder Sachbeschädigung schützen. Des Weiteren SOLLTE hierbei berücksichtigt werden, welche Informationen und IT-Systeme in den Fahrzeugen aufbewahrt werden dürfen. Ausreichende Maßnahmen zum Zutrittsschutz SOLLTEN ergriffen werden.

Die Ladung der Fahrzeuge SOLLTE sicher verstaut werden. Es SOLLTE sichergestellt werden, dass schützenswerte Informationen nicht von außerhalb der Fahrzeuge von Unbefugten eingesehen, mitgehört oder entwendet werden können. Die Mitarbeitenden SOLLTEN mit der grundlegenden Funktionsweise der Fahrzeuge und den betreffenden IT-Komponenten vertraut gemacht werden. Die Mitarbeitenden SOLLTEN auch über die bestehenden Sicherheitsrisiken informiert werden.

INF.11.A8 Schutz vor witterungsbedingten Einflüssen (S) [Benutzende, Fachverantwortliche]

Fahrzeuge und die darin verbauten IT-Komponenten SOLLTEN vor witterungsbedingten Einflüssen ausreichend geschützt werden. Je nach Fahrzeugart, Einsatzort und Einsatzumgebung SOLLTEN zusätzliche Schutzmaßnahmen ergriffen werden. Für kurzfristig auftretende extreme Wettererscheinungen SOLLTEN entsprechende Schutzmaßnahmen getroffen werden.

Diese Schutzmaßnahmen SOLLTEN in den Handlungsanweisungen zur Fahrzeugbenutzung in Form von Checklisten dokumentiert werden.

INF.11.A9 Sicherstellung der Versorgung (S) [Fachverantwortliche]

Bevor Fahrzeuge eingesetzt werden, SOLLTE geplant werden, wie diese mit Betriebsstoffen während des Einsatzes versorgt werden. Die Fahrzeuge SOLLTEN dabei während des Einsatzes immer ausreichend mit Betriebsstoffen versorgt werden.

INF.11.A10 Aussonderung (S) [IT-Betrieb, Fachverantwortliche]

Werden Fahrzeuge ausgesondert, SOLLTEN keine schützenswerten Informationen in den Fahrzeugen verbleiben. Bevor Fahrzeuge endgültig ausgesondert werden, SOLLTE anhand der Inventarliste geprüft werden, ob keine inventarisierten Gegenstände und darüber hinaus relevanten Gegenstände zurückgelassen worden sind.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.11.A11 Ersatzvorkehrungen bei Ausfällen (H) [Fachverantwortliche]

Für den Fall, dass Fahrzeuge oder Fahrzeugführende ausfallen, SOLLTEN innerhalb der Institution vorbereitende Maßnahmen getroffen werden. Abhängig von der Bedeutung der Fahrzeuge SOLLTEN Ersatzfahrzeuge bereitstehen oder alternativ ein Rahmenvertrag mit einer geeigneten Fremdinstitution geschlossen werden. Zusätzlich dazu SOLLTEN Ersatzfahrzeugführende verfügbar sein.

INF.11.A12 Diebstahlsicherung bzw. Bewachung (H) [Fachverantwortliche, Mitarbeitende]

Eine Alarmanlage SOLLTE vorhanden sein. Bei Bodenfahrzeugen SOLLTE darüber hinaus eine Wegfahrsperre vorhanden sein. Wird das Fahrzeug verlassen, SOLLTEN die Alarmanlage und Wegfahrsperre aktiviert werden. Alternativ SOLLTEN die Fahrzeuge bewacht werden.

INF.11.A13 Schädigende Fremdeinwirkung (H) [Fachverantwortliche]

Je nach Art der Fahrzeuge SOLLTEN geeignete Maßnahmen ergriffen werden, um die Fahrzeuge vor potentieller Fremdeinwirkung in der geplanten Einsatzumgebung zu schützen, wie z. B. störenden Funkstrahlen.

INF.11.A14 Schutz sensibler Informationen vor unbefugtem Zugriff und Kenntnisnahme (H) [IT-Betrieb, Fachverantwortliche]

Fahrzeuge und die dazugehörigen IT-Komponenten SOLLTEN so abgesichert werden, dass sensible Informationen durch Unbefugte nicht ausgelesen bzw. manipuliert oder gelöscht werden können. Hierbei SOLLTEN die vorhandenen Schutzvorkehrungen der herstellenden Unternehmen überprüft und bei Bedarf angepasst werden.

INF.11.A15 Physische Absicherung der Schnittstellen (H) [IT-Betrieb, Fachverantwortliche]

Alle physischen internen und externen Schnittstellen der Fahrzeuge SOLLTEN physisch gegen unbefugte Benutzung und äußere Einflüsse abgesichert werden.

INF.11.A16 Brandlöschanlage (H) [Fachverantwortliche]

Die Fahrzeuge SOLLTEN über eine Brandlöschanlage verfügen, die einen Brand von außen und innen löschen kann. Alternativ SOLLTEN geeignete Mittel zur Brandbekämpfung mitgeführt werden.

INF.11.A17 Netztrennung des In-Vehicle-Network mit einem Sonderfahrzeugnetz über Gateways (H)

Generell SOLLTE die Institution sicherstellen, dass keine Informationen unerlaubt und undefiniert zwischen

- dem In-Vehicle-Network (IVN), das wiederum an die Netze der fahrzeugherstellenden Unternehmen angebunden ist und
- den einsatzspezifischen IT-Komponenten

ausgetauscht werden. Hierzu SOLLTEN Gateways mit standardisierten Protokollen (z. B. nach Standard CiA 447) eingesetzt werden. Die Gateways SOLLTEN dabei vom fahrzeugherstellenden Unternehmen freigegeben sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Der wissenschaftliche Artikel „IT-Sicherheit und Datenschutz im vernetzten Fahrzeug“ des Fraunhofer Instituts (DOI: 10.1007/s11623-015-0434-4) gibt einen generellen Überblick über vernetzte Fahrzeuge, mögliche Anwendungen, die benötigten Daten und die sich daraus ergebenden Bedrohungen.

Der wissenschaftliche Artikel „Security Issues and Vulnerabilities in Connected Car Systems“ von der IEEE Konferenz 2015 zeigt auf, welche neuen Bedrohungen durch die Fahrzeugvernetzung entstehen.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.12 Verkabelung

1. Beschreibung

1.1. Einleitung

Die ordnungsgemäße und normgerechte Ausführung der Verkabelung ist Grundlage für einen sicheren IT-Betrieb. Dabei muss grundsätzlich zwischen der elektrotechnischen Verkabelung und der IT-Verkabelung unterschieden werden.

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers (VNB) bis zu den Anschlüssen der Endgeräte.

Die IT-Verkabelung in einer Institution umfasst alle Kommunikationskabel und passiven Komponenten wie Rangier- bzw. Spleißverteiler oder Patchfelder. Sie bildet also die physikalische Grundlage der internen Kommunikationsnetze. Die IT-Verkabelung reicht von den Übergabepunkten aus einem Fremdnetz bis zu den Anschlusspunkten der Netzteilnehmenden. Übergabepunkte sind z. B. der Anschluss eines Telekommunikationsunternehmens oder die DSL-Anbindung eines Internet-Providers.

Trotz dieser Unterscheidung sind die grundlegenden Anforderungen an beide Arten der Verkabelung identisch. Daher sollte die Verkabelung innerhalb einer Institution immer auch als Ganzes betrachtet werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die gesamte elektrotechnische Verkabelung und IT-Verkabelung vor Ausfall, Manipulation und Störung zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein INF.12 *Verkabelung* ist einmal auf die Verkabelung in Gebäuden und Räumen anzuwenden, zusätzlich zum Baustein INF.1 *Allgemeines Gebäude*. Die Anforderungen des Bausteins sind immer sowohl auf die IT- als auch auf die elektronische Verkabelung anzuwenden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.12 *Verkabelung* von besonderer Bedeutung.

2.1. Kabelbrand

Kabelbrände können einen Informationsverbund erheblich schädigen. Ein Kabelbrand verursacht z. B. Kurzschlüsse oder unterbricht Leiter. Infolgedessen fallen auch Schutzeinrichtungen aus. Zudem können bei Kabelbränden, abhängig von den Materialien der Isolierungen, aggressive Gase entstehen.

2.2. Unzureichende Dimensionierung der Verkabelung

Werden Arbeitsplätze, Serverräume oder Rechenzentren geplant, dann werden diese Pläne häufig ausschließlich am aktuellen Bedarf ausgerichtet. Jedoch verlangen zukünftige neue Anforderungen oft auch nach weiteren Kapazitäten des Stromnetzes und der Datenkabel. Dies kann z. B. notwendig werden, sobald zusätzliche Server eingesetzt werden oder sich technische Standards ändern. Die Verkabelung kann aber nur in dem Umfang erweitert werden, den die bereits vorhandenen und verlegten Kabel und Kabeltrassen zulassen.

2.3. Unzureichende Dokumentation der Verkabelung

Wenn die genaue Lage von Kabeln nicht bekannt ist, weil sie unzureichend dokumentiert wurde, dann können diese Kabel bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes beschädigt werden. Eine unzureichende Dokumentation erschwert es auch, Kabel zu prüfen und zu reparieren.

Darüber hinaus kann nicht davon ausgegangen werden, dass alle Kabel in den Installationszonen nach aktuell gültigen Normen installiert sind.

2.4. Unzureichend geschützte Verteiler

Gelegentlich sind Verteilungen des Stromversorgungs- oder Datennetzes unverschlossen in Bereichen installiert, die allgemein zugänglich sind. Unbefugte Personen können solche Verteiler öffnen, manipulieren und so Ausfälle in der Strom- oder Datenversorgung herbeizuführen.

2.5. Leitungsbeschädigungen

Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr, dass es absichtlich oder unabsichtlich beschädigt wird. Beschädigungen verursachen nicht nur direkte Ausfälle von Verbindungen, sondern können auch später zu Störungen führen. Eine beschädigte Isolierung beeinträchtigt unter Umständen erst mit großer zeitlicher Verzögerung die funktionellen Eigenschaften eines Kabels.

2.6. Spannungsschwankungen, Überspannung, Unterspannung

Schwankungen der Versorgungsspannung können in allen Bereichen der Netze entstehen. Extrem kurze und kleine Ereignisse wirken sich kaum oder gar nicht auf IT-Systeme aus. Größere Schwankungen führen jedoch zu Funktionsstörungen. Die angeschlossenen Systeme können beschädigt werden bis hin zu Totalausfällen. Auch zerstörerische Überspannungen können auftreten.

2.7. Verwendung qualitativ unzureichender Steckdosenleisten

Oft reichen die fest installierten Steckdosen für die zu betreibenden Geräte nicht aus. Um dies auszugleichen, werden häufig Steckdosenleisten verwendet. Sind diese Steckdosenleisten jedoch qualitativ unzureichend, dann können sie zur Zündquelle und damit zu einer großen Brandgefahr werden.

In vielen Fällen werden mehrere Steckdosenleisten hintereinander geschaltet, um Steckplätze für alle Geräte bereitzustellen. Bei einer solchen Reihenschaltung besteht die Gefahr der Überlastung. Die Folge kann ein unvollständiger Kurzschluss mit hoher Brandgefahr sein.

2.8. Unzulässige Kabelverbindungen

In manchen Fällen werden zwischen IT-Systemen oder anderen technischen Komponenten Kabelverbindungen hergestellt, die nicht vorgesehen und unzulässig sind. Dies kann Sicherheitsprobleme oder Betriebsstörungen verursachen.

So ermöglichen solche Kabelverbindungen unter Umständen, dass unerlaubt auf Datennetze, IT-Systeme, Informationen oder Anwendungen zugegriffen werden kann. Durch unzulässige Kabelverbindungen können Informationen auch zu falschen Empfangenden übertragen werden. Zudem kann die Verbindung gestört werden.

2.9. Leitungsbeeinträchtigungen

Die elektrische Signalübertragung in Kommunikationskabeln kann durch elektrische und magnetische Felder negativ beeinflusst werden. Eine spezielle Form dieser Leitungsbeeinträchtigung ist Übersprechen. Dabei werden Ströme und Spannungen von benachbarten Leitungen als Störsignale auf das Kommunikationskabel übertragen.

2.10. Abhören und Manipulation von Kabeln

Abhörangriffe auf Datenkabel sind eine Gefahr für die Informationssicherheit, die nicht vernachlässigt werden sollte. Grundsätzlich gibt es keine abhörsicheren Kabel. Die Kabel unterscheiden sich in ihrer Qualität lediglich hinsichtlich des Aufwands, der zum Abhören der Leitung betrieben werden muss. Ob ein Kabel tatsächlich abgehört wird, ist nur mit hohem messtechnischem Aufwand feststellbar.

Daneben stellen bewusste Manipulationen von Kabeln bis hin zu ihrer Zerstörung eine Gefahr für die Institution dar. Fehlfunktionen von Kabeln können in manipulativer Absicht bewusst herbeigeführt werden. Solche Manipulationen verfolgen oftmals das Ziel, den IT-Betrieb zu stören oder die Institution zu schädigen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.12 *Verkabelung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	IT-Betrieb, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.12.A1 Auswahl geeigneter Kabeltypen (B) [IT-Betrieb, Haustechnik]

Bei der Auswahl von Kabeltypen MUSS geprüft werden, welche übertragungstechnischen Eigenschaften notwendig sind. Die einschlägigen Normen und Vorschriften MÜSSEN beachtet werden. Auch die Umgebungsbedingungen im Betrieb und bei der Verlegung MÜSSEN berücksichtigt werden. Hinsichtlich der Umgebungsbedingungen MÜSSEN die folgenden Faktoren beachtet werden:

- Temperaturen,
- Kabelwege,
- Zugkräfte bei der Verlegung,
- die Art der Verlegung sowie
- die Entfernung zwischen den Endpunkten und möglichen Störquellen.

INF.12.A2 Planung der Kabelführung (B) [IT-Betrieb, Haustechnik]

Kabel, Kabelwege und Kabeltrassen MÜSSEN aus funktionaler und aus physikalischer Sicht ausreichend dimensioniert werden. Dabei MÜSSEN künftige Notwendigkeiten eingerechnet werden, z. B. genügend Platz für mögliche technische Erweiterungen in Kabelkanälen und -trassen. Bei der gemeinsamen Führung von IT- und Stromverkabelung in einer Trasse MUSS das Übersprechen zwischen den einzelnen Kabeln verhindert werden. Es MUSS darauf geachtet werden, dass die IT-Verkabelung und die elektrotechnische Verkabelung mit dem normgerechten Trennungsabstand geführt werden. Erkennbare Gefahrenquellen MÜSSEN umgangen werden.

INF.12.A3 Fachgerechte Installation (B) [IT-Betrieb, Haustechnik]

Die Installationsarbeiten der Verkabelung MÜSSEN fachkundig und sorgfältig erfolgen. Bei der Installation MÜSSEN alle relevanten Normen beachtet werden. Die fachgerechte Ausführung der Verkabelung MUSS durch eine fachkundige Person in allen Phasen überprüft werden. Bei Anlieferung des Materials MUSS geprüft werden, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Es MUSS darauf geachtet werden, dass die Montage keine Beschädigungen verursacht. Außerdem MÜSSEN die Kabelwege so gewählt werden, dass eine Beschädigung der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen ist.

INF.12.A4 EMV-taugliche Stromversorgung (B) [Haustechnik]

Die Stromversorgung MUSS EMV (Elektromagnetische Verträglichkeit) -tauglich sein. Dafür MUSS das Stromverteilnetz als TN-S-System aufgebaut sein. Bei Aufbau und Betrieb des Stromverteilnetzes MÜSSEN die in den entsprechenden Normen empfohlenen Trennungsabstände soweit wie möglich eingehalten werden. Vorkehrungen gegen Einstrahlungen von außen, Abstrahlung durch die Stromleitung sowie zur Erkennung von Ausgleichsströmen MÜSSEN getroffen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.12.A5 Anforderungsanalyse für die Verkabelung (S) [IT-Betrieb, Haustechnik]

Grundsätzlich SOLLTEN die Anforderungen analysiert werden, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der Verkabelung haben. In dieser Anforderungsanalyse SOLLTE zunächst abgeschätzt werden, wie die kurzfristige Nutzung der Verkabelung innerhalb der Institution aussieht. Darauf aufbauend SOLLTE die längerfristige Entwicklung der Nutzung abgeschätzt werden. Darüber hinaus MÜSSEN die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit bei der Anforderungsanalyse für die Verkabelung mit betrachtet werden.

INF.12.A6 Abnahme der Verkabelung (S) [IT-Betrieb, Haustechnik]

Für die Verkabelung SOLLTE es einen Abnahmeprozess geben. Verkabelungen SOLLTEN immer dann abgenommen werden, wenn alle (gegebenenfalls im Rahmen eines Meilensteins) durchzuführenden Aufgaben abgeschlossen sind. Die Ausführenden SOLLTEN hierfür die Aufgaben als abgeschlossen und zur Abnahme bereit gemeldet haben. Außerdem SOLLTEN sich bei den Kontrollen durch die auftraggebende Institution keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin SOLLTE so gewählt werden, dass die Kontrollen zur Abnahme in ausreichender Zeit vorbereitet werden können. Die auftragnehmende Institution MUSS spätestens zum Abnahmetermin schriftlich belegen, dass sämtliche Normen und Vorschriften eingehalten wurden, die für das Gewerk gelten. Bei der Abnahme MUSS der tatsächliche Umfang der Leistungen überprüft werden. Für das Abnahmeprotokoll SOLLTE eine Checkliste vorbereitet werden. Das Abnahmeprotokoll MUSS von den Teilnehmenden und Verantwortlichen rechtsverbindlich unterzeichnet werden. Das Protokoll MUSS Bestandteil der internen Dokumentation der Verkabelung sein.

INF.12.A7 Überspannungsschutz (S) [Haustechnik]

Jedes elektrisch leitende Netz SOLLTE gegen Überspannungen geschützt werden. Hierfür MUSS ein entsprechendes Überspannungsschutzkonzept erstellt werden, das den gültigen Normen entspricht. Netzersatzanlagen (NEA) und unterbrechungsfreie Stromversorgungen (USV) MÜSSEN in das Überspannungsschutzkonzept aufgenommen werden.

INF.12.A8 Entfernen und Deaktivieren nicht mehr benötigter Kabel (S) [IT-Betrieb, Haustechnik]

Wenn Kabel nicht mehr benötigt werden, SOLLTEN sie fachgerecht und vollständig entfernt werden. Nachdem Kabel entfernt wurden, MÜSSEN die Brandschottungen fachgerecht verschlossen werden.

Kabel, die aktuell nicht mehr benötigt werden, aber mit der vorhandenen Technik sinnvoll als Reserve an Ort und Stelle verbleiben können, SOLLTEN in einem betriebsfähigen Zustand erhalten werden. Solche Kabel MÜSSEN mindestens an den Endpunkten entsprechend gekennzeichnet werden.

Grundsätzlich SOLLTE eine Übersicht über nicht mehr benötigte Kabel aufgestellt werden. Aus der Dokumentation SOLLTE hervorgehen, welche Kabel entfernt oder deaktiviert wurden.

INF.12.A9 Brandschutz in Trassen (S) [Haustechnik]

Trassen SOLLTEN ausreichend dimensioniert werden. Trassen SOLLTEN über eine ausreichende Be- und Entlüftung verfügen.

INF.12.A10 Dokumentation und Kennzeichnung der Verkabelung (S) [IT-Betrieb, Haustechnik]

Eine Institution SOLLTE sicherstellen, dass sie für ihre Verkabelung sowohl über eine interne als auch eine externe Dokumentation verfügt. Die interne Dokumentation MUSS alle Aufzeichnungen zur Installation und zum Betrieb der Verkabelung enthalten. Die interne Dokumentation SOLLTE so umfangreich angefertigt und gepflegt werden, dass der Betrieb und dessen Weiterentwicklung bestmöglich unterstützt werden. Die externe Dokumentation (Beschriftung von Anschlüssen zur Unterstützung des Betriebs) der Verkabelung SOLLTE möglichst neutral gehalten werden.

Jede Veränderung im Netz SOLLTE dokumentiert werden. Eine Interims- oder Arbeitsversion der Dokumentation SOLLTE unmittelbar, d. h. am Tag selbst angepasst werden. Die Stamm-Dokumentation MUSS spätestens 4 Wochen nach Abschluss der jeweiligen Arbeiten aktualisiert sein. Es SOLLTE geprüft werden, ob ein Dokumentenmanagement für die Dokumentation eingesetzt werden kann. Die Dokumentation SOLLTE regelmäßig überprüft und aktualisiert werden. Sämtliche technischen Einrichtungen, die im Rahmen der Verkabelung dokumentiert sind, MÜSSEN hinsichtlich der Dokumentationstreue spätestens nach 4 Jahren geprüft werden.

INF.12.A11 Neutrale Dokumentation in den Verteilern (S) [IT-Betrieb, Haustechnik]

In jedem Verteiler SOLLTE es eine Dokumentation geben, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Die Dokumentation im Verteiler MUSS ein sicheres Schalten ermöglichen.

Die Dokumentation im Verteiler SOLLTE möglichst neutral gehalten werden. In der Dokumentation im Verteiler SOLLTEN nur bestehende und genutzte Verbindungen sowie auflaufende Reservekabel aufgeführt sein. Falls möglich, SOLLTEN keine Hinweise auf die Art gegeben werden, wie Kabel genutzt werden. Es SOLLTEN nur solche Hinweise gegeben werden, die ausdrücklich vorgeschrieben sind. Alle weitergehenden Informationen SOLLTEN in einer Revisionsdokumentation aufgeführt werden.

INF.12.A12 Kontrolle elektrotechnischer Anlagen und bestehender Verbindungen (S) [IT-Betrieb, Haustechnik]

Alle elektrischen Anlagen und Betriebsmittel SOLLTEN gemäß DGUV Vorschrift 3, entsprechend den in § 5 Prüfung genannten Durchführungsanweisungen, regelmäßig geprüft werden. Alle Unregelmäßigkeiten, die festgestellt werden, MÜSSEN unverzüglich dokumentiert werden. Festgestellte Unregelmäßigkeiten MÜSSEN unverzüglich den zuständigen Organisationseinheiten gemeldet werden. Die zuständigen Organisationseinheiten MÜSSEN die festgestellten Unregelmäßigkeiten so zeitnah beheben, dass eine Gefährdung von Personen ausgeschlossen werden kann. Die Verfügbarkeit der elektrischen Anlagen und Betriebsmittel MUSS hierbei im erforderlichen Maß sichergestellt sein.

INF.12.A13 Vermeidung elektrischer Zündquellen (S) [Haustechnik]

Die Nutzung privater Elektrogeräte innerhalb einer Institution SOLLTE klar geregelt werden. Alle Elektrogeräte MÜSSEN durch eine Elektrofachkraft geprüft und für sicher befunden werden, bevor sie eingesetzt werden. Die Verwendung von Steckdosenleisten SOLLTE soweit wie möglich vermieden werden. Fehlende Steckdosen SOLLTEN durch eine Elektrofachkraft fachgerecht nachgerüstet werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.12.A14 A-B-Versorgung (H) [Haustechnik]

Es SOLLTE geprüft werden, ob anstelle einer einzügigen Stromversorgung eine zweizügige sogenannte A-B-Versorgung geschaffen werden soll, die wichtige IT-Komponenten und andere Verbraucher versorgt. Dabei SOLLTE die Funktionsfähigkeit der Stromversorgung permanent durch geeignete technische Einrichtungen überwacht werden.

INF.12.A15 Materielle Sicherung der Verkabelung (H) [IT-Betrieb, Haustechnik]

Für alle Räume eines Gebäudes, insbesondere in Räumen mit Publikumsverkehr sowie in unübersichtlichen Bereichen SOLLTE überlegt werden, Kabel und Verteiler gegen unbefugte Zugriffe zu sichern. In jedem Fall SOLLTEN die

Zahl und der Umfang derjenigen Stellen möglichst gering gehalten werden, an denen Einrichtungen der Energieversorgung und Zugangspunkte des Datennetzes für Unbefugte zugänglich sind.

INF.12.A16 Nutzung von Schranksystemen (H) [Haustechnik]

Elektrotechnische Anschlüsse und -verteiler SOLLTEN in Schranksystemen aufgestellt oder in diese eingebaut werden. Bei der Dimensionierung der Schranksysteme SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.

INF.12.A17 Redundanzen für die IT-Verkabelung (H) [IT-Betrieb]

Es SOLLTE geprüft werden, ob eine redundante primäre IT-Verkabelung geschaffen werden soll, die über unabhängige Trassen geführt wird. Ebenso SOLLTE geprüft werden, ob die Anschlüsse an IT- oder TK-Provider redundant ausgelegt werden sollen. Bei hohen oder sehr hohen Verfügbarkeitsanforderungen SOLLTE überlegt werden, in den relevanten Gebäuden die Sekundär- und Tertiärverkabelung redundant auszulegen. Dabei SOLLTEN redundant ausgelegte Teile der Sekundärverkabelung in unterschiedlichen Brandabschnitten geführt werden. Wird eine redundante Verkabelung verwendet, SOLLTE deren Funktionsfähigkeit regelmäßig geprüft werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Deutsche Institut für Normung formuliert Vorgaben, die für die Verkabelung relevant sind. Hierbei handelt es sich um folgende Normen:

- DIN 4102, Brandverhalten von Baustoffen und Bauteilen
- DIN IEC 60364, Einrichten von Niederspannungsanlagen
- IEC 62305, Merkblatt: Die Blitzschutz-Normen DIN EN 62305 / VE 01805-305:2006
- IN VDE 0100, Errichten von Niederspannungsanlagen
- DIN VDE 0105-100, Betrieb von elektrischen Anlagen
- DIN 41494, Bauweisen für elektronische Einrichtungen
- DIN EN 50173, Informationstechnik – Anwendungsneutrale Kommunikationskabelanlagen
- DIN EN 50174, Informationstechnik – Installation von Kommunikationsverkabelung
- DIN EN 50310:2017-02, Telekommunikationstechnische Potentialausgleichsanlage für Gebäude und andere Strukturen
- DIN EN 50346:2010-02, Informationstechnik – Installation von Kommunikationsverkabelung – Prüfen installierter Verkabelung
- DIN IEC 60297, Bauweise für elektronische Einrichtungen

Die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW) hat in der DGUV Vorschrift 3: „Elektrische Anlagen und Betriebsmittel, Unfallverhütungsvorschrift“ weitere Vorschriften für die elektrotechnische Verkabelung veröffentlicht.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 11801:2002-09 „Informationstechnik – Anwendungsneutrale Standortverkabelung“ Vorgaben für die IT-Verkabelung.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.13 Technisches Gebäudemanagement

1. Beschreibung

1.1. Einleitung

Das Gebäudemanagement (GM), auch Facility Management genannt, ist für alle Leistungen zuständig, die in der Planungs- und Nutzungsphase von Gebäuden, Gebäudekomplexen, Liegenschaften oder Liegenschaftsportfolios anfallen. Im Folgenden wird hierfür einheitlich der Begriff Gebäude genutzt. Ausnahmen hiervon werden explizit genannt.

Das GM ist standort- sowie objektbezogen ausgerichtet. Es lässt sich in technisches, infrastrukturelles und kaufmännisches GM untergliedern.

Das technische Gebäudemanagement (TGM) umfasst gemäß DIN 32736 alle Leistungen, die die technische Funktion und Verfügbarkeit eines Gebäudes erhalten. Zu diesen Leistungen gehören unter anderem:

- Betreiben
- Dokumentieren
- Energie- und Umweltmanagement
- Informationsmanagement
- Modernisieren
- Sanieren
- Umbauen
- Verfolgen der technischen Gewährleistung

Wesentliche technische Funktionen eines Gebäudes werden durch die technische Gebäudeausrüstung (TGA) bereitgestellt, die durch das TGM betrieben, gepflegt und weiterentwickelt wird. Die TGA umfasst dabei gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen (siehe auch Kapitel 4.1 *Genutzte TGM-spezifische Fachbegriffe*). Falls die TGA automatisiert und gewerkübergreifend betrieben werden soll, wird zusätzliche technische Infrastruktur zur Gebäudeautomation (GA, engl. Building Automation and Control Systems, BACS) eingesetzt. Somit ist die GA ein zentrales Werkzeug des TGM. Ein Gebäude kann durch TGM auch ohne GA betrieben werden, GA hingegen ist immer durch TGM flankiert. Gewisse Komponenten der GA sind dabei auch der TGA zuzurechnen, wie z. B. echtzeitfähige Industrial Ethernet Switches.

Während die TGA in der Vergangenheit meist unabhängig von der IT und der Prozessleit- und Automatisierungstechnik (Operational Technology, OT) betrieben wurde, werden heute zunehmend Netzübergänge zu diesen Bereichen etabliert. Hinzu kommt, dass Teile der TGA rund um die Uhr genutzt werden. Daher müssen Änderungen oft parallel zur produktiven Nutzung durchgeführt werden.

Auch im TGM müssen die Grundwerte der Informationssicherheit berücksichtigt werden, denn der Verlust von Verfügbarkeit, Vertraulichkeit und Integrität von Systemen kann im TGM weitreichende Auswirkungen bis hin zur Gefährdung von Leib und Leben nach sich ziehen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Umsetzung und Betrieb im Rahmen des TGM zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein INF.13 *Technisches Gebäudemanagement* ist auf das TGM einer Institution anzuwenden, sobald Gebäude mit TGA geplant, gebaut oder betrieben werden.

Dieser Baustein behandelt das TGM, somit die Aufgaben und Prozesse, die für die Planung und den Betrieb der TGA-Anlagen (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe) eines Gebäudes erforderlich sind. Die technische Infrastruktur für den automatisierten Betrieb von Gebäuden wird im Baustein INF.14 *Gebäudeautomation* behandelt. Letzterer muss zusätzlich zum Baustein INF.13 *Technisches Gebäudemanagement* angewendet werden, wenn die zu betreibende TGA automatisiert und anlagenübergreifend gesteuert wird. In diesem Sinne umfasst das TGM auch die Prozesse der GA.

Weiterhin ist es möglich, dass zu den zu verwaltenden Systemen auch solche gehören, die durch Bausteine aus den Schichten IND *Industrielle IT* und SYS *IT-Systeme* modelliert werden, z. B. IND.2.1 *Allgemeine ICS-Komponente* oder auch SYS.4.4 *Allgemeines IoT-Gerät*. Darüber hinaus müssen die für das TGM relevanten Aspekte der Schichten ORP und OPS beachtet werden, insbesondere die Teilschichten OPS.1 *Eigener Betrieb* und OPS.2 *Betrieb von Dritten* sowie die Bausteine ORP.2 *Personal* und ORP.4 *Identitäts- und Berechtigungsmanagement*. Werden für das TGM Cloud-Dienste eingesetzt, muss für die Auswahl dieser Dienste der Baustein OPS.2.2 *Cloud-Nutzung* berücksichtigt werden.

Zur Absicherung von Fernzugängen im TGM sind die Bausteine OPS.1.2.5 *Fernwartung* und IND.3.2 *Fernwartung im industriellen Umfeld* anzuwenden.

Der Baustein INF.13 *Technisches Gebäudemanagement* behandelt nicht die physische Sicherheit von Gebäuden, diese wird in dem Baustein INF.1 *Allgemeines Gebäude* behandelt. Ebenso spielt der Aspekt der Safety in diesem Baustein keine hervorgehobene Rolle, sondern wird im Baustein IND.2.7 *Safety Instrumented Systems* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.13 *Technisches Gebäudemanagement* von besonderer Bedeutung.

2.1. Fehlende Grundlagen für die Planung des TGM

Wenn beim Bau eines Gebäudes die Nachfrageorganisationen (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe) noch nicht feststehen, fehlen Kontaktpersonen, Zielsetzung und Bedarfe für das TGM. Das kann dazu führen, dass das TGM im Betrieb nicht dem tatsächlichen Bedarf entspricht, weil dieser zum Zeitpunkt der Planung und Umsetzung nicht abgefragt werden konnte.

2.2. Mangelnde Dokumentation beim TGM

In das TGM ist häufig eine Vielzahl von Dienstleistenden involviert. Ist die Dokumentation der Zuständigkeiten mit Kontaktpersonen und zugehörigen SLAs unvollständig oder nicht zugänglich, führt dies im Ernstfall, wenn wichtige Systeme ausfallen, zu vermeidbaren Verzögerungen, die gegebenenfalls sogar Personenschaden zur Folge haben können.

Eine fehlende Dokumentation von Sicherheitszertifizierungen der TGA-Anlagen inklusive Terminen für notwendige Erneuerung kann dazu führen, dass abgelaufene Zertifizierungen nicht rechtzeitig erneuert werden. Dadurch kann gegen Gesetze verstoßen werden, je nach TGA-Anlage Gefahr für Leib und Leben entstehen und ein entstandener Schaden nicht über entsprechende Versicherungen abgewickelt werden.

2.3. Kompromittierung der Schnittstellen mit TGM

Das TGM hat technische Schnittstellen zu besonders schützenswerten Bereichen, z. B. Safety Instrumented Systems (SIS), Sicherheitsdienst und Brandmeldeanlagen. Wenn diese Schnittstellen bewusst oder unbewusst durch Fehler im TGM kompromittiert werden, dann kann dies einen Verstoß gegen Gesetze sowie Gefahr für Leib und Leben zur Folge haben.

Wird z. B. bei einem Feueralarm in einem Rechenzentrum die optische oder akustische Warnung außer Kraft gesetzt, können im Raum befindliche Personen diesen nicht rechtzeitig verlassen, bevor der Raum mit Löschgas geflu-

tet wird. Ebenso kann ein vorgetäuschter Feueralarm dazu führen, dass Fluchttüren geöffnet werden und dadurch unberechtigter Zugang erlangt wird oder Türen geschlossen und gegebenenfalls Personen eingeschlossen werden.

2.4. Unzureichendes Monitoring der TGA

Wenn die TGA nur unzureichend durch ein entsprechendes Monitoring überwacht wird, dann werden sicherheitsrelevante Ereignisse, wie z. B. relevante Fehlfunktionen in der TGA, unter Umständen nicht oder zu spät erkannt. Dies kann je nach Ereignis zu weiteren Schäden führen oder Gefahr für Leib und Leben bedeuten.

Wird z. B. der Ausfall der Heizung bei Außentemperaturen im Minusbereich nicht gemeldet, kühlen die Räume erst stark aus, bevor der Ausfall bemerkt wird und eine Behebung eingeleitet werden kann.

2.5. Unzureichendes Rollen- und Berechtigungsmanagement

Wenn das TGM oder einzelne seiner Teile von der restlichen IT der Institution physisch getrennt werden, dann wird in der Regel auch ein dediziertes Identitäts- und Berechtigungsmanagement eingerichtet. Wenn dieses unzureichend konzipiert und umgesetzt wird, dann kann nicht ausgeschlossen werden, dass mehrere Personen dasselbe Konto nutzen oder Berechtigungen von ausgeschiedenen internen oder externen Mitarbeitenden oder Dienstleistenden nicht gelöscht wurden. Als Folge kann auf das TGM unberechtigt zugegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.13 *Technisches Gebäudemanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Haustechnik
Weitere Zuständigkeiten	Planende, IT-Betrieb, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.13.A1 Beurteilung des Ist-Zustands bei der Übernahme bestehender Gebäude (B)

Bei der Übernahme von bestehenden Gebäuden MÜSSEN die im Gebäude installierten TGA-Anlagen, die Bausubstanz und Einrichtungen sowie vorhandene Dokumentation erfasst und hinsichtlich ihres Zustands (Alter, Supportstatus, Zukunftsfähigkeit, Vollständigkeit der Dokumentation etc.) beurteilt werden.

INF.13.A2 Regelung und Dokumentation von Verantwortlichkeiten und Zuständigkeiten im Gebäude (B) [Institutionsleitung, Planende]

Da es in einem Gebäude meist unterschiedliche Verantwortlichkeiten und Zuständigkeiten für verschiedene Bereiche gibt, MÜSSEN die entsprechenden Rechte, Pflichten, Aufgaben, Kompetenzen und zugehörigen Prozesse geregelt und dokumentiert werden.

Hierbei MÜSSEN auch die organisatorischen Strukturen im Gebäude berücksichtigt und dokumentiert werden. Insbesondere MÜSSEN alle Nachfrage- und betreibenden Organisationen erfasst werden. Wird das TGM durch eine externe Organisation betrieben, MÜSSEN die zugehörigen Rechte, Pflichten, Aufgaben und Kompetenzen gemäß Baustein OPS.2.3 *Nutzung von Outsourcing* vertraglich festgehalten werden.

Weiterhin MÜSSEN die Schnittstellen und Meldewege inklusive Eskalation zwischen allen Beteiligten festgelegt und dokumentiert werden. Auch die Koordination verschiedener betreibender Organisationen MUSS geregelt und dokumentiert werden.

Der Zugriff auf die Dokumentation MUSS geregelt werden. Die gesamte Dokumentation inklusive der zugehörigen Kontaktinformationen MUSS immer aktuell und verfügbar sein.

INF.13.A3 Dokumentation von Gebäudeeinrichtungen (B)

Alle Gebäudeeinrichtungen der TGA inklusive GA MÜSSEN dokumentiert werden. Hierbei MUSS sämtliche, auch schon vorhandene, Dokumentation zusammengeführt, aus dem Blickwinkel des TGM organisiert und um TGM-spezifische Angaben ergänzt werden.

Der Zugriff auf die Dokumentation MUSS geregelt werden. Die gesamte Dokumentation inklusive der zugehörigen Kontaktinformationen MUSS immer aktuell und verfügbar sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.13.A4 Erstellung einer Sicherheitsrichtlinie für TGM (S)

Ausgehend von der allgemeinen Sicherheitsleitlinie der Institution SOLLTE eine übergeordnete Sicherheitsrichtlinie für TGM erstellt sowie nachvollziehbar umgesetzt werden. Aus dieser übergeordneten Sicherheitsrichtlinie SOLLTEN spezifische Sicherheitsrichtlinien für die verschiedenen Themenbereiche des TGM abgeleitet werden. In der Sicherheitsrichtlinie für das TGM SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie das TGM umgesetzt wird. Die Sicherheitsrichtlinie SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können. Sie SOLLTE allen im Bereich TGM zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein.

INF.13.A5 Planung des TGM (S) [Planende]

Das TGM, die zugrundeliegende Infrastruktur und die zugehörigen Prozesse SOLLTEN geeignet geplant werden. Die Planung SOLLTE dabei mindestens eine detaillierte Anforderungsanalyse, eine ausreichende Grobkonzeptionierung und eine Fein- und Umsetzungsplanung umfassen.

Im Rahmen der Anforderungsanalyse SOLLTEN Anforderungen an TGM-Infrastruktur und TGM-Prozesse spezifiziert werden. Dabei SOLLTEN alle wesentlichen Elemente für das TGM berücksichtigt werden. Auch SOLLTE die Sicherheitsrichtlinie für das TGM beachtet werden. Steht die Nachfrageorganisation zum Zeitpunkt der Planung noch nicht fest, SOLLTEN im Rahmen einer universellen Planung zumindest grundlegende Anforderungen erfasst werden, die dem Stand der Technik entsprechen.

Für die Anforderungsspezifikation SOLLTEN auch die Schnittstellen der zu verwaltenden Systeme dokumentiert werden, z. B. um die Kompatibilität von TGM-Lösung und zu verwaltenden Systemen zu gewährleisten.

Außerdem SOLLTEN vor der Beauftragung von Dienstleistenden oder vor der Anschaffung von Hard- oder Software der durch das TGM zu verwaltenden Systeme die Anforderungen des TGM in einem Lastenheft des TGM spezifiziert werden. In diesem Lastenheft SOLLTE auch die Durchführung von Tests berücksichtigt werden (siehe auch INF.13.A22 *Durchführung von Systemtests im TGM*).

Wenn im TGM Funktionen der Künstlichen Intelligenz (KI) eingesetzt werden, SOLLTE bei dem zuständigen herstellenden Unternehmen angefragt werden, ob und wie die Informationssicherheit hier angemessen berücksichtigt wird.

Die Grobkonzeptionierung SOLLTE gemäß INF.13.A6 *Erstellung eines TGM-Konzepts* erfolgen.

In der Fein- und Umsetzungsplanung für das TGM SOLLTEN alle in der Sicherheitsrichtlinie und im TGM-Konzept adressierten Punkte berücksichtigt werden.

INF.13.A6 Erstellung eines TGM-Konzepts (S) [Planende]

Ausgehend von der Sicherheitsrichtlinie für das TGM SOLLTE ein TGM-Konzept erstellt und gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das TGM
- Absicherung des Zugangs und der Kommunikation
- Absicherung auf Ebene des Netzes, insbesondere Zuordnung von TGM-Komponenten zu Netzsegmenten
- Umfang des Monitorings und der Alarmierung
- Protokollierung von Ereignissen und administrativen Zugriffen
- Meldeketten bei Störungen und Sicherheitsvorfällen
- benötigte Prozesse für das TGM
- Bereitstellung von TGM-Informationen für andere Betriebsbereiche
- Einbindung des TGM in die Notfallplanung

Das TGM-Konzept SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neue Erkenntnisse abdecken zu können.

Außerdem SOLLTE regelmäßig ein Soll-Ist-Vergleich zwischen den Vorgaben des Konzepts und dem aktuellen Zustand durchgeführt werden. Dabei SOLLTE insbesondere geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.

INF.13.A7 Erstellung eines Funkfrequenzkatasters (S)

Um Funkfrequenzen weitestgehend störungsfrei nutzen zu können, SOLLTE ein Funkfrequenzkataster erstellt werden, dass die Systeme und Nutzenden des Frequenzspektrums an den Standorten der Institution listet. Dabei SOLLTE bei einer potentiellen Nutzung von Frequenzen durch unterschiedliche Systeme und Nutzende festgelegt werden, wer auf welchen Frequenzen der Primärnutzende ist. Dabei SOLLTE auch eine Abstimmung zwischen IT und TGM erfolgen. Wird in den Gebäuden OT eingesetzt, SOLLTE auch hier eine Abstimmung erfolgen.

Das Funkfrequenzkataster SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden.

INF.13.A8 Erstellung und Pflege eines Inventars für das TGM (S) [Planende]

Für die Dokumentation von Systemen, die durch das TGM verwaltet werden, SOLLTE ein Inventar erstellt und gepflegt werden. Das Inventar SOLLTE vollständig und aktuell gehalten werden. Aus dem Inventar SOLLTEN für alle Systeme Verantwortlichkeiten und Zuständigkeiten ersichtlich sein.

Auch die Elemente der TGM-Infrastruktur selbst SOLLTEN dokumentiert werden.

INF.13.A9 Regelung des Einsatzes von Computer-Aided Facility Management (S) [Planende]

Wird ein Computer-Aided Facility Management-System (CAFM-System) eingesetzt, SOLLTE dieser Einsatz umfassend geplant und konzeptioniert werden. Werden im CAFM Prozesse abgebildet und unterstützt, SOLLTEN entsprechende Rollen und Berechtigungen definiert werden, insbesondere wenn externe Dienstleistende an den Prozessen beteiligt sind.

INF.13.A10 Regelung des Einsatzes von Building Information Modeling (S) [Planende]

Soweit möglich SOLLTE Building Information Modeling (BIM) zur digitalen Modellierung aller relevanten Gebäudedaten eingesetzt werden. Bei der Verwendung von BIM SOLLTE der BIM-Projektabwicklungsplan spezifiziert werden.

Weiterhin SOLLTE die BIM-Architektur umfassend geplant und konzeptioniert werden. Auch für die BIM-Werkzeuge SOLLTE die Informationssicherheit angemessen gewährleistet werden.

INF.13.A11 Angemessene Härtung von Systemen im TGM (S)

Alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTEN angemessen gehärtet werden. Die Härtungsmaßnahmen SOLLTEN dokumentiert, regelmäßig und zusätzlich bei Bedarf überprüft und, falls erforderlich, angepasst werden.

Für alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTE bei der Beschaffung sichergestellt werden, dass diese angemessen gehärtet werden können und insbesondere sicherheitsrelevante Updates für die geplante Nutzungsdauer bereitgestellt werden.

Systeme, für die keine sicherheitsrelevanten Updates verfügbar sind, SOLLTEN nach Bekanntwerden von Schwachstellen nicht mehr genutzt werden. Wenn dies nicht möglich ist, SOLLTEN die betroffenen Systeme mit den Mitteln der Netzsegmentierung separiert und die Kommunikation kontrolliert und reglementiert werden.

INF.13.A12 Sichere Konfiguration der TGM-Systeme (S)

Alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTEN sicher konfiguriert werden.

Die Konfiguration SOLLTE mindestens vor Inbetriebnahme eines Systems getestet werden. Konfigurationsänderungen während des Produktivbetriebs SOLLTEN vor Aktivierung auf einer Testinstanz getestet oder nur im Vier-Augen-Prinzip durchgeführt werden.

Die Konfiguration von Systemen SOLLTE gesichert werden, um ein schnelles Wiedereinspielen einer fehlerfreien Version zu ermöglichen (Rollback). Rollback-Tests SOLLTEN auf einem Testsystem eingerichtet oder während Wartungsfenstern durchgeführt werden. Die Konfigurationen SOLLTEN zentral gespeichert werden.

Für gleichartige Systeme, inklusive der Geräte der Automations- und Feldebene (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe), SOLLTE eine automatisierte Verteilung von Software-Updates und Konfigurationen eingerichtet werden.

Konfigurationsänderungen SOLLTEN allen Beteiligten an Betriebs- und Serviceprozessen (Entstörung, Rufbereitschaft, Wartungen etc.) bekannt gemacht werden, insbesondere

- Änderungen der Zugangsmechanismen oder der Passwörter sowie
- Änderungen an Kommunikations- und Steuerparametern für die eingebundenen Systeme.

Es SOLLTE sichergestellt werden, dass im Störungsfall beispielsweise eine Wartungstechnikerin oder ein Wartungstechniker das System bedienen bzw. parametrieren kann.

Außerdem SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen von den Vorgaben SOLLTEN behoben werden.

INF.13.A13 Sichere Anbindung von eingeschränkt vertrauenswürdigen Systemen im TGM (S) [Planende]

Eingeschränkt vertrauenswürdige Systeme, die aus wichtigen betrieblichen Gründen im TGM eingebunden werden müssen, SOLLTEN über ein System angebunden werden, das die Kommunikation mit Hilfe von Firewall-Funktionen kontrolliert und reglementiert. Dieses System SOLLTE in der Verantwortlichkeit des TGM liegen.

INF.13.A14 Berücksichtigung spezieller Rollen und Berechtigungen im TGM (S)

Im Rollen- und Berechtigungskonzept hinsichtlich des TGM SOLLTEN sowohl Nachfrage- als auch betreibende Organisationen der TGM-Systeme und der TGA-Systeme berücksichtigt werden. Dies SOLLTE insbesondere dann sorgfältig geplant werden, wenn das TGM institutionsübergreifend bereitgestellt wird.

INF.13.A15 Schutz vor Schadsoftware im TGM (S)

Können auf einem System keine Virenschutzprogramme gemäß Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ausgeführt werden, beispielsweise aufgrund von knappen Ressourcen oder aufgrund von Echtzeitanforderungen, SOLLTEN geeignete alternative Schutzverfahren eingesetzt werden.

Jedes externe System und jeder externe Datenträger SOLLTE vor der Verbindung mit einem TGM-System und vor der Datenübertragung auf Schadsoftware geprüft werden.

INF.13.A16 Prozess für Änderungen im TGM (S)

Änderungen SOLLTEN immer angekündigt und mit allen beteiligten Gewerken (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe), Nachfrage- und betreibenden Organisationen abgestimmt werden. Außerdem SOLLTEN Regelungen für den Fall getroffen werden, dass ein Rückbau von Änderungen mit fehlerhaftem Ergebnis nicht oder nur mit hohem Aufwand möglich ist. Daher sollten im Änderungsmanagement vor Ausführung der Änderung Tests durchgeführt werden, die auch die Fähigkeit des Rückbaus beinhalten. Für die verschiedenen Typen von Änderungen SOLLTE die jeweilige Testtiefe festgelegt werden. Bei der Einführung neuer Systeme und bei großen Änderungen an bestehenden Systemen SOLLTE eine entsprechend hohe Testtiefe vorgesehen werden (siehe INF.13.A22 *Durchführung von Systemtests im TGM*).

INF.13.A17 Regelung von Wartungs- und Reparaturarbeiten im TGM (S)

Gebäudeeinrichtungen SOLLTEN regelmäßig gewartet werden. Hierfür SOLLTE ein Wartungsplan erstellt werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind. Dabei SOLLTEN auch die Abhängigkeiten der verschiedenen Gewerke berücksichtigt werden. Darüber hinaus SOLLTE festgelegt werden, wer für die Wartung oder Reparatur von Einrichtungen zuständig ist. Durchgeführte Wartungsarbeiten SOLLTEN dokumentiert werden.

Es SOLLTE zu jedem Zeitpunkt gewährleistet werden, dass Wartungs- und Reparaturarbeiten, die durch Dritte ausgeführt werden, kontrolliert, ausschließlich abgestimmt durchgeführt und abgenommen werden. Hierfür SOLLTEN interne Mitarbeitende der Haustechnik bestimmt werden, die solche Wartungs- und Reparaturarbeiten autorisieren, beobachten, gegebenenfalls unterstützen und abnehmen.

INF.13.A18 Proaktive Instandhaltung im TGM (S) [Planende]

Für Systeme, die durch das TGM verwaltet werden, SOLLTE eine angemessene proaktive Instandhaltung durchgeführt werden. Hierfür SOLLTEN die regelmäßigen Wartungsintervalle je System festgelegt werden. Zusätzlich SOLLTE je System abgewogen werden, ob ergänzend zur regelmäßigen Instandhaltung eine vorausschauende Instandhaltung (engl. Predictive Maintenance) genutzt werden kann und in welchem Umfang hierdurch die regelmäßigen Wartungsintervalle verlängert werden können.

INF.13.A19 Konzeptionierung und Durchführung des Monitorings im TGM (S) [Planende]

Es SOLLTE ein Konzept für das Monitoring im TGM erstellt und umgesetzt werden. Darin SOLLTE spezifiziert werden, wie die durch das TGM zu verwaltenden Systeme in ein möglichst einheitliches Monitoring eingebunden werden können und welche Werte überwacht werden sollten. Hierfür SOLLTEN schon bei der Anforderungsanalyse erforderliche Schnittstellen für das Monitoring wichtiger Zustände von Systemen spezifiziert werden, die durch das TGM verwaltet werden. Außerdem SOLLTEN auch die für das TGM genutzten Systeme in das Monitoring eingebunden werden.

Das Konzept SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

Statusmeldungen und Monitoringdaten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

INF.13.A20 Regelung des Ereignismanagements im TGM (S) [Planende]

Im TGM auftretende Ereignisse SOLLTEN hinsichtlich ihrer Bedeutung und ihres Einflusses kategorisiert, gefiltert und klassifiziert werden (englisch Event Management). Für die Ereignisse SOLLTEN Schwellwerte definiert werden, die eine automatisierte Einstufung von Ereignissen ermöglichen. Je nach Klassifizierung der Ereignisse SOLLTEN entsprechende Maßnahmen für Monitoring, Alarmierung und Meldewege (Eskalation) sowie Maßnahmen zur Protokollierung bestimmt werden.

INF.13.A21 Protokollierung im TGM (S)

Ereignisse, die im Ereignismanagement entsprechend klassifiziert wurden, SOLLTEN protokolliert werden. Außerdem SOLLTEN für die Systeme sicherheitsrelevante Ereignisse protokolliert werden.

Alle Konfigurationszugriffe sowie alle manuellen und automatisierten Steuerungszugriffe SOLLTEN protokolliert werden. Abhängig vom Schutzbedarf SOLLTE eine vollumfängliche Protokollierung inklusive Metadaten und Inhalt der Änderungen erfolgen.

Die Protokollierung SOLLTE auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

Bei sicherheitskritischen Ereignissen SOLLTE automatisch alarmiert werden.

INF.13.A22 Durchführung von Systemtests im TGM (S) [Planende]

Systeme des TGM und Systeme, die durch das TGM verwaltet werden, SOLLTEN vor der Inbetriebnahme und bei großen Systemänderungen hinsichtlich ihrer funktionalen und nicht-funktionalen Anforderungen getestet werden. Dabei SOLLTE auch das Soll- und Ist-Verhalten von Funktionen und Einstellungen geprüft werden. Bei den nicht-funktionalen Anforderungen SOLLTEN auch Anforderungen der Informationssicherheit getestet sowie zusätzlich bei Bedarf auch Lasttests durchgeführt werden. Für die Tests SOLLTE eine Testspezifikation erstellt werden, die eine Beschreibung der Testumgebung, der Testtiefe und der Testfälle inklusive der Kriterien für eine erfolgreiche Testdurchführung enthält. Die Testdurchführung SOLLTE in einem Testbericht dokumentiert werden.

Testspezifikationen SOLLTEN regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

INF.13.A23 Integration des TGM in das Schwachstellenmanagement (S)

Systeme des TGM und die durch das TGM verwalteten Systeme SOLLTEN fortlaufend hinsichtlich möglicher Schwachstellen überwacht werden.

Hierfür SOLLTEN regelmäßig Informationen über bekanntgewordene Schwachstellen eingeholt und entsprechend berücksichtigt werden. Hierbei SOLLTE auch die Konfiguration der Systeme dahingehend überprüft werden, ob sie bekannt gewordene Schwachstellen begünstigt.

Weiterhin SOLLTE entschieden werden, für welche Systeme regelmäßig oder zumindest bei Inbetriebnahme und bei großen Systemänderungen Schwachstellen-Scans durchgeführt werden. Für Schwachstellen-Scans SOLLTE die Scan-Tiefe festgelegt werden. Außerdem SOLLTE festgelegt werden, ob ein passiver oder ein aktiver Scan durchgeführt wird. In Produktivumgebungen SOLLTEN passive Scans bevorzugt werden. Aktive Scans SOLLTEN in Produktivumgebungen nur durchgeführt werden, wenn sie notwendig sind und Personal hinzugezogen wird, das durch den Scan bedingte, eventuell auftretende Fehler oder Ausfälle beheben kann.

INF.13.A24 Sicherstellung der Kontrolle über die Prozesse bei Cloud-Nutzung für das TGM (S) [Planende]

Werden im TGM Cloud-basierte Dienste genutzt, SOLLTE die Kontrolle über alle TGM-Prozesse im TGM verbleiben. Dies SOLLTE bei Nutzung eines Cloud-Dienstes vertraglich mit dem anbietenden Unternehmen festgelegt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.13.A25 Aufbau einer Testumgebung für das TGM (H) [Planende]

Bei erhöhtem Schutzbedarf SOLLTE für Systeme des TGM und für Systeme, die durch das TGM verwaltet werden, eine Testumgebung eingerichtet werden, damit Hard- und Software vor der Inbetriebnahme und bei Änderungen getestet und Fehler im produktiven Betrieb reduziert werden können. Außerdem SOLLTEN Regelungen für den Umgang mit Systemen spezifiziert werden, für die keine Testumgebung aufgebaut werden kann.

INF.13.A26 Absicherung von BIM (H) [Planende]

Werden in BIM auch sicherheitskritische Informationen erfasst, SOLLTEN sowohl auf Ebene der BIM-Architektur als auch für Implementierung und Betrieb der BIM-Lösung entsprechende Sicherheits- und Härtungsmaßnahmen vorgesehen werden. Die Absicherung SOLLTE ein verschärftes Rollen- und Berechtigungskonzept sowie weitergehende Schutzmaßnahmen wie Verschlüsselung, Segmentierung und höherwertige Authentisierungsmechanismen, insbesondere eine 2-Faktor-Authentisierung, beinhalten.

INF.13.A27 Einrichtung einer Private Cloud für das TGM (H) [Planende]

Bei erhöhtem Schutzbedarf SOLLTEN Cloud-Dienste zum TGM in einer Private Cloud On-Premises oder einer Private Cloud bei einem vertrauenswürdigen Anbietenden positioniert werden. Der Einsatz einer Public Cloud SOLLTE vermieden werden.

INF.13.A28 Sichere Nutzung von Künstlicher Intelligenz im TGM (H)

Werden bei erhöhtem Schutzbedarf im TGM Funktionen der Künstlichen Intelligenz (KI) genutzt, SOLLTE nur eine KI genutzt werden, die nachweislich sicher ist. Mindestens SOLLTE darauf geachtet werden, dass keine Daten in Netze geleitet werden, die nicht zur eigenen Institution gehören oder nicht vertrauenswürdig sind.

Für Cloud-basierte KI-Dienste SOLLTEN über die Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* hinaus auch die Kriterien des AI Cloud Service Compliance Criteria Catalogue (AIC4) des BSI berücksichtigt werden.

INF.13.A29 Integration des TGM in ein SIEM (H) [IT-Betrieb]

Wird ein System für das Security Information and Event Management (SIEM) genutzt, SOLLTEN die Systeme des TGM und soweit möglich auch die durch das TGM verwalteten Systeme entsprechend eingebunden werden, um system- und anwendungsübergreifende sicherheitsrelevante Vorfälle erkennen und analysieren zu können.

INF.13.A30 Durchführung von Penetrationstests im TGM (H)

Um Systeme des TGM und Systeme, die durch das TGM verwaltet werden, entsprechend abzusichern, SOLLTEN bedarfsorientiert Penetrationstests durchgeführt werden. Mindestens SOLLTEN vor der Inbetriebnahme und bei großen Systemänderungen in einer Testumgebung Penetrationstests durchgeführt werden.

Werden im TGM Funktionen der KI genutzt, SOLLTEN diese in die Penetrationstests einbezogen werden.

4. Weiterführende Informationen

4.1. Genutzte TGM-spezifische Fachbegriffe

Automationsebene

Die Automationsebene befindet sich in der Automatisierungspyramide zwischen der Feldebene und der Managementebene. Sie führt die von der Feldebene gelieferten Daten sowie die von der Managementebene übermittelten Vorgaben zusammen. Hier erfolgt die Steuerung und Regelung der TGA-Anlagen, aber auch die Überwachung von Grenzwerten, Schaltzuständen oder Zählerständen.

Building Information Modeling (BIM)

Gemäß VDI 2552 Blatt 2 ist BIM eine Methodik zur Planung, zur Ausführung und zum Betrieb von Bauwerken mit einem kollaborativen Ansatz auf Grundlage eines digitalen Informationsmodells des Bauwerks zur gemeinschaftlichen Nutzung.

Computer-Aided Facility Management (CAFM)

Gemäß VDI 3814 Blatt 2.1 dient CAFM als Werkzeug zur Erfassung, Verarbeitung, Aufbereitung und Archivierung von Daten und Informationen mit dem Ziel, die Leistungsprozesse und Aufgaben in der Betriebsphase eines Gebäudes zu unterstützen.

Feldebene

Die Feldebene stellt die unterste Ebene der Automatisierungspyramide dar und umfasst unterschiedliche Komponenten der GA oder OT. In der Regel werden hier Sensoren und Aktoren betrieben. Sensoren erfassen Informationen (z. B. Bewegung, Helligkeit, Temperatur) und senden diese an die Automationsebene. Aktoren empfangen Steuerinformationen und setzen diese in Schaltsignale um, z. B. für die Beleuchtungs-, Heizungs-, Klima- und Lüftungsanlage.

Gebäude

Der Begriff Gebäude wird im Baustein INF.13 *Technisches Gebäudemanagement* und in den zugehörigen Umsetzungshinweisen synonym für Gebäude, Gebäudekomplex, Liegenschaft und Liegenschaftsportfolio genutzt. Außerdem beschreibt der Begriff Gebäude nicht nur Häuser und Hallen, sondern auch beispielsweise einen Fernsehturm oder eine Bohrinsel.

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

Die Gebäudeautomation (GA) umfasst gemäß VDI 3814-1 alle Produkte und Dienstleistungen zum zielsetzungsgerichteten Betrieb der Technischen Gebäudeausrüstung.

Gebäudekomplex

Ein Gebäudekomplex ist eine Gruppe von Gebäuden, die baulich miteinander verbunden sind und als Gesamteinheit wahrgenommen werden.

Gewerk

Im Bauwesen umfasst ein Gewerk im Allgemeinen die Arbeiten, die einem in sich geschlossenen Bauleistungsbereich zuzuordnen sind. Es handelt sich um einen Funktionsbereich, der insbesondere verschiedene TGA-Anlagen umfassen kann.

Beispiel: Raumlufttechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlagen und Kälteanlagen gehören.

Leitstand (englisch Control Center)

Ein Leitstand (auch Bedien- und Beobachtungseinheiten) ist ein technisches Werkzeug zur Visualisierung aktueller Abläufe, Zustände und Situationen von Prozessen, inklusive TGM- und speziell GA-Prozesse.

Liegenschaft

Eine Liegenschaft ist ein Grundstück inklusive seiner Bebauung. Zur Bebauung gehören alle unbeweglichen Sachen, d. h. Gebäude und sonstige Dinge, die nicht ohne Weiteres vom Grundstück entfernt werden können.

Liegenschaftsportfolio

Als Liegenschaftsportfolio wird die Gesamtheit der Liegenschaften im Besitzstand bezeichnet.

Nachfrageorganisation

Eine Nachfrageorganisation ist gemäß DIN EN ISO 41011 eine Organisationseinheit innerhalb oder außerhalb der Institution, die für ihre Erfordernisse autorisiert ist, entsprechende Anforderungen an TGA, GA oder TGM zu stellen und die Kosten zur Erfüllung der Anforderungen zu übernehmen.

Beispiele: Mietparteien innerhalb eines Gebäudes, Eigentümerinnen und Eigentümer eines Gebäudes, Dienstleistende innerhalb einer Institution, z. B. Kantine.

System

Der Begriff System adressiert im Baustein INF.13 *Technisches Gebäudemanagement* und in den zugehörigen Umsetzungshinweisen nicht nur ein IT-System im klassischen Sinn (vergleiche Bausteine der Schicht SYS), sondern umfasst auch alle Komponenten der TGA einschließlich aller Komponenten der Feldebene, wie Sensoren, Aktoren usw.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der Gebäudeautomation sind ebenfalls zur TGA zuzurechnen, z. B. echtzeitfähige Industrial Ethernet Switches.

Technisches Gebäudemanagement (englisch Technical Building Management, TBM)

Das Technische Gebäudemanagement (TGM) beinhaltet gemäß DIN 32736 alle Leistungen, die zum Erhalt der technischen Funktion und Verfügbarkeit eines Gebäudes dienen. Das TGM übernimmt somit für die TGA das Betreiben, Instandhalten, Modernisieren und Dokumentieren der Komponenten und definiert alle notwendigen Prozesse.

TGA-Anlage

Eine Anlage der TGA beschreibt die Gesamtheit aller zur Erfüllung bestimmter Funktionen zusammenwirkenden technischen Komponenten. Beispiele gemäß DIN 276 „Kosten im Bauwesen" sind Wärmeversorgungsanlagen, Lüftungsanlagen oder Beleuchtungsanlagen.

4.2. Abkürzungen

Abkürzung	Bedeutung
AI	Artificial Intelligence
AIC4	AI Cloud Service Compliance Criteria Catalogue
BACS	Building Automation and Control Systems
BIM	Building Information Modelling
BS	Building Services
CAFM	Computer-Aided Facility Management
DIN	Deutsches Institut für Normung
GA	Gebäudeautomation
GM	Gebäudemanagement
ICS	Industrial Control System
KI	Künstliche Intelligenz
OT	Operational Technology
SIEM	Security Information and Event Management
SIS	Safety Instrumented Systems
SLA	Service Level Agreement
TBM	Technical Building Management
TGA	Technische Gebäude-Ausstattung
TGM	Technisches Gebäude-Management
VDI	Verein Deutscher Ingenieure e.V.

4.3. Wissenswertes

Genannte Normen und Dokumente:

- AI Cloud Service Compliance Criteria Catalogue (AIC4), Bundesamt für Sicherheit in der Informationstechnik, Februar 2021, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html
- BSI-CS 108 – Fernwartung im industriellen Umfeld, BSI Veröffentlichung zur Cyber-Sicherheit, Juli 2018, aufrufbar über https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf?__blob=publicationFile
- DIN 276 – Kosten im Bauwesen, Deutsches Institut für Normung e.V., Dezember 2018, verfügbar im Beuth-Verlag
- DIN 32736 – Gebäudemanagement – Begriffe und Leistungen, Deutsches Institut für Normung, August 2000, verfügbar im Beuth-Verlag
- VDI 4700 Blatt 1 – Begriffe der Bau- und Gebäudetechnik, Verein Deutscher Ingenieure e.V., Oktober 2015, verfügbar im Beuth-Verlag

Bundesamt
für Sicherheit in der
Informationstechnik

INF.14 Gebäudeautomation

1. Beschreibung

1.1. Einleitung

Die Gebäudeautomation (GA, englisch Building Automation and Control Systems, BACS) automatisiert den gewerkübergreifenden Betrieb von Gebäuden ganz oder teilweise und stellt hierfür die technische Infrastruktur zur Verfügung. Wesentliche technische Funktionen eines Gebäudes werden durch die technische Gebäudeausrüstung (TGA) bereitgestellt, die mit den Leistungen des technischen Gebäudemanagements (TGM) betrieben, gepflegt und weiterentwickelt werden. Die GA ist somit ein zentrales Werkzeug des TGM, um für den Gebäudebetrieb die gesetzte Zielrichtung umzusetzen. Sie umfasst alle Produkte und Dienstleistungen zum übergreifenden, automatisierten Betrieb der TGA. Kriterien für die Zielrichtung können Funktionalität, Energieeffizienz und Nachhaltigkeit, Sicherheit, Verfügbarkeit oder Komfort sein. Die GA kann auf Leistungen für Gebäude, Gebäudekomplexe, Liegenschaften oder Liegenschaftsportfolios skaliert werden. Im Folgenden wird hierfür einheitlich der Begriff Gebäude genutzt. Ausnahmen hiervon werden explizit genannt.

Die GA führt unter anderem Automatisierungsaufgaben wie automatisiertes Messen, Steuern und Regeln (MSR) sowie Aufgaben für Monitoring, Service und Diagnose, Optimierung, Bedienung und Management für die TGA eines Gebäudes durch.

Die GA wird innerhalb eines Gebäudes für eine oder gegebenenfalls mehrere Nachfrageorganisationen, beispielsweise Mietparteien, bereitgestellt. Hierfür wird die TGA meist separat für verschiedene GA-Bereiche, beispielsweise für Nachfrageorganisationen oder für Gebäudeteile, gesteuert.

In einem Gebäude kann die GA abhängig von der genutzten TGA durch mehrere parallele GA-Systeme umgesetzt werden. Ein GA-System stellt die technische Realisierung der GA dar und kann auch übergreifend für mehrere Gebäude innerhalb eines Gebäudekomplexes oder einer Liegenschaft genutzt werden. Verschiedene GA-Systeme können kooperieren, aber auch vollständig unabhängig voneinander betrieben werden.

Während die TGA in der Vergangenheit oft nicht übergreifend automatisiert betrieben wurde, werden heute zunehmend GA-Systeme zur übergeordneten, gewerkübergreifenden Steuerung der TGA genutzt. Hierfür werden zunehmend auch Techniken genutzt, die ursprünglich nur in der Informationstechnik (IT) und der industriellen Prozessleit- und Automatisierungstechnik (Operational Technology, OT) verwendet wurden, z. B. eine Kommunikation via Internet und Cloud-Diensten.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Realisierung und Betrieb von GA zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein INF.14 *Gebäudeautomation* ist auf die GA einer Institution anzuwenden, sobald die TGA in Gebäuden mittels GA gesteuert wird. Der Baustein ist nur auf die Schnittstellen der GA zu den TGA-Anlagen anzuwenden, die TGA-Anlagen mit den anlageninternen Netzen und Netzstrukturen sind nicht im Fokus dieses Bausteins.

Der Baustein INF.14 *Gebäudeautomation* behandelt Systeme und Leistungen, die zu beachten und zu erfüllen sind, wenn die GA, gegebenenfalls bestehend aus mehreren GA-Systemen, geplant, aufgebaut und betrieben wird. Hierbei werden auch spezifische Gegebenheiten behandelt, die für Netze und Netzkomponenten der GA gelten.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Die allgemeinen Anforderungen für GA und TGA, die nicht überwiegenden Aspekte für ein übergreifendes, automatisiertes Messen, Steuern und Regeln thematisieren, werden im Baustein INF.13 *Technisches Gebäudemanagement* behandelt. Dieser ist stets mitzubetrachten.
- Anforderungen an die allgemeine Infrastruktur, insbesondere Gebäude und Räume bzw. Arbeitsplätze, werden in den Bausteinen der Schicht INF *Infrastruktur* behandelt (z. B. Baustein INF.1 *Allgemeines Gebäude*).
- Werden Teile der GA, die für eine Institution erforderlich sind, von einer anderen Institution, z. B. von Dienstleistenden in der Rolle als Gebäudebetreibende (betreibende Organisation), erbracht, so muss für die Bereitstellung und den Betrieb der GA der Baustein OPS.2.3 *Nutzung von Outsourcing* angewendet werden.
- Spezifische Anforderungen an GA-Komponenten, die auch für den Bereich der industriellen IT oder OT genutzt werden können, werden in den Bausteinen der Schicht IND *Industrielle IT* thematisiert (siehe z. B. Baustein IND.2.3 *Sensoren und Aktoren* oder Baustein IND.2.7 *Safety Instrumented Systems*).
- Der Baustein NET.1.1 *Netzarchitektur und -design* behandelt die grundsätzlichen Aspekte für Netze, wie sie neben der Büro-IT auch in der GA und der industriellen IT anwendbar sind. Generelle Anforderungen an die Absicherung von Netzkomponenten behandeln die Bausteine in NET.3 *Netzkomponenten* (z. B. Baustein NET.3.1 *Router und Switches*).
- Außerdem sind alle passenden organisatorischen und technischen Bausteine für Server und Anwendungen anzuwenden. Beispielsweise ist für den Fernzugriff auf die GA-Komponenten der Baustein OPS.1.2.5 *Fernwartung* anzuwenden.
- Erfolgt die Vernetzung von Gebäuden Cloud-basiert, so ist zusätzlich der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.14 *Gebäudeautomation* von besonderer Bedeutung.

2.1. Unzureichende Planung der GA

Die GA dient der koordinierten, übergreifenden Steuerung der Anlagen der TGA. Eine unzureichende Planung der GA kann damit zu Sach- oder Vermögensschäden und im schlimmsten Fall zu Personenschäden führen.

Dies kann beispielsweise dann passieren, wenn durch unzureichende Redundanzplanung das zentrale Steuersystem einer Vereinzelungsanlage ausfällt und Personen in einer Schleuse eingeschlossen werden.

Die beschriebene Gefährdungslage verschärft sich in der GA zudem durch die Komplexität der Planung. Hier sind heterogene Gruppen von TGA-Anlagen (Gewerke) sowie eine Vielzahl unterschiedlicher Dienstleistenden und GA-Bereiche zu berücksichtigen.

2.2. Fehlerhafte Integration von TGA-Anlagen in die GA

Die GA steuert die Anlagen der TGA übergreifend. Ist nur eine Anlage fehlerhaft oder unzureichend integriert, kann die Funktionalität der gesamten GA eingeschränkt werden.

Beispielsweise können eingehende Meldungen falsch interpretiert werden oder Meldungen erreichen die GA nicht, so dass die GA falsch oder gar nicht reagiert. Werden beispielsweise die Informationen der Zugangskontrollanlage nicht korrekt oder gar nicht empfangen, können Heizung und Beschattung für die entsprechenden Räume gegebenenfalls nicht angemessen gesteuert werden.

2.3. Nutzung unsicherer Systeme und Protokolle in der GA

In den durch die GA gesteuerten TGA-Anlagen werden häufig Komponenten genutzt, die z. B. aufgrund ihres Alters keine Aktualisierungen mehr erhalten, Schwachstellen aufweisen bzw. nicht mehr dem aktuellen Stand der Technik entsprechen. Dies resultiert oft aus einer unzureichenden Qualität in den Entwicklungs- und Wartungspro-